通信情報保護學會誌
第 10 券 第 4 號, 2000. 12

인증서 관리 프로토콜(CMP)의 최근 동향

류 종 호*, 염 흥 열*

요 약

본 논문에서는 PKI(Public Key Infrastructure)의 주요 응용 프로토콜 중에서, 인증서를 발급하고 발급된 인증서를 전달하는 절차, 인증기관간의 믿음을 확장하기 위한 상호 인증과 관련된 절차, 인증기관이 인증서를 발급 받는 최종개체의 공개키에 대응되는 개인키를 소유하고 있음을 증명하는 개인키 소유 증명(POP : Proof Of Propession)절차, 인증기관의 암호키 생신을 위한 절차 등과 같은 인증서에 대한 관리 프로토콜(CMP : Certificate Management Protocol)에 대하여 중점적으로 논의 하고자 한다.

Ⅰ. 서 론

안전한 전자거래를 위해서는 인증서비스가 절대적으로 요구된다. 인증기관의 인증서비스가 제공되지 않는 온라인 전자결재, 전자계약 등과 같은 온라인 거래는 상대적으로 미약한 신뢰성이 갖게 된다. 따라서 보다 안전한 거래를 형성하기 위해서는 현재 법률적 문서 체계에서 공식적인 법적 계약에 이용되는 인감과 동등한 효력을 지닌 인증 서비스를 이용하는 것이 보다 확실한 방법일 것이다.

국내에서는 인터넷 등 개방형 정보통신망을 이용하여 처리되는 전자문서의 안전/신뢰성을 확보하고 그 이용을 활성화하기 위하여 전자서명 인증 관리 체계 및 국가 전체의 공개키 기반구조 구축·운영에 관한 기본적인 사항을 정함으로써 국가 사회의 정보화를 촉진할 목적으로 1999년 2월 5일 전자서명법(법률 제5792호)이 제정되어 1999년 7월 1일부터 시행되고 있다.

전자서명법은 비대칭형 공개키 암호기술을 기반으로 하는 전자서명이며 개인의 법인감과 동일한 효력을 부여함으로서, 컴퓨터 네트워크를 이용한 온라인 전자거래를 활성화 할 수 있는 제도적 기반 마련을 하였다고 볼 수 있다. 이에 따라 전자거래에 목적을 둔 이용자들은 법적 효력을 갖는 전자서명을 수행하기 위해서 필히 공인된 인증기관으로부터 자신의 전자서명 검증키에 대한 인증서를 발급 받아야 한다. 전자서명법은 기존의 종이에 이루어진 서명을 전자적으로 수행될 수 있게 하는 중요한 법적 제도적 체계를 마련했다고 할 수 있다.

본 논문에서는 PKI(Public Key Infrastructure)의 주요 응용 프로토콜 중에서, 인증서를 발급하고 발급된 인증서를 전달하는 절차, 인증기관간의 믿음을 확장하기 위한 상호 인증과 관련된 절차, 인증기관이 인증서를 발급 받는 최종개체의 공개키에 대응되는 개인키를 소유하고 있음을 증명하는 개인키 소유 증명(POP : Proof Of Propession)절차, 인증기관의 암호키 생신을 위한 절차 등과 같은 인증서에 대한 관리 프로토콜(CMP : Certificate Management Protocol)에 대하여 중점적으로 논의 하고자 한다.

최근에 IETF(Internet Engineering Task Force)에서는 인증서 관리 프로토콜 규격을 RFC 2510으로 표준화하였다. 따라서 이를 활용한 인증서 관리 프로토콜이 앞으로 일반화 될 것이다.

본 논문의 II 장에서는 PKI 개체들과 PKI 관리 요구 사항, 그리고 관리의 가정 및 제한에 대하여 논 할 것이고, III 장에서는 인증서 관리를 위한 주요 기능, 인증서 발급을 위한 두 가지 초기 등록/인

* 순천향대학교

증 방법, 개인키 소유 증명, 인증기관의 암호키 쌍의 갱신, 그리고 인증서 관리 메시지의 구성와 같은 필수 PKI 관리 기능들에 대하여 논 할 것이다. 마지막으로 IV 장에서 결론을 내린다.

II. 공개키 기반구조 관리 개요

PKI는 관리하는 개인들의 유형에 일치하도록 구성되어야 한다. 관리자에게 무한한 선택을 제공하면 소프트웨어를 복잡하게 할 뿐 아니라 관리자나 소프트웨어 개발자에 의한 미묘한 실수가 넓은 타협(compromise)를 초래할 것이다. 반대로 복잡한 메커니즘으로 관리자의 제어 분야를 제한하게 된다면 그들이 PKI를 사용하지 않는 결과를 초래할 수도 있게 된다.

또한 관리 프로토콜은 반드시 PKI 구성 요소들간에 온라인 상호동작(interactive)을 지원해야 한다. 예를 들어 관리 프로토콜은 키 쌍이 연관되는 인증기관과 클라이언트간에 사용될 수 있으며 서로 인증서를 발행하는 인증기관간에도 사용될 수 있기 때문에, 상호 참여자간에 일치되는 채널 동작이 요구된다.

PKI 관리 형태는 일반적으로 특정의 메시지 형태나 절차를 규정하기 전에 PKI 관리와 연관되는 개체들과 그들의 상호동작들을 정의한 이후, 확인 가능한 최종개체들의 유형을 확인하기 위해 이들 기능들을 그룹화하여 구성된다.

1. PKI 개체들

PKI 관리와 연관되는 개체들은 인증서의 주체필드의 이름을 갖는 최종개체와 인증서의 발행자필드의 이름을 갖는 인증기관(CA: Certification Authority)으로 구성된다. 등록기관(RA : Registration Authority)은 주체와 인증기관간의 중간 매개체로 이 역시 PKI 관리에 개입한다.

인증서 관리 프로토콜을 위한 구성 시스템은 그림 1과 같이 최종개체에게 인증서를 발행하는 인증기관, 인증기관의 일부 기능인 신분확인 기능을 대신하는 등록기관, 인증기관에게 인증서 발행을 요구하고 발행된 인증서를 수신하는 최종개체(EE : End Entity), 그리고 인증서와 인증서 취소 목록을 저장하는 저장소(Repository)들로 구성된다.

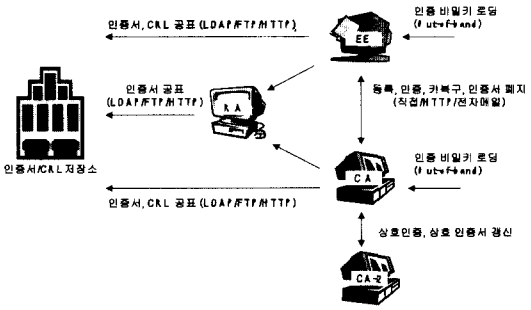


그림 1. 인증서 관리 요소 시스템 및 관리 동작

- 주체와 최종개체 : 주체(Subject)는 인증서의 subject 필드에 입력되는 개체를 나타낸다. 최종 개체는 사용자와 응용을 포함하는 개체를 지칭한다. 최종개체의 PSE(Personal Security Enviroment)는 최종개체의 이름, 최종개체의 공개키와 개인키, 자신이 믿는 루트 인증기관의 공개키 등을 저장하고 있는 안전한 국부 메모리를 지칭한다.

- 인증기관(CA) : 여기서 인증서 관리를 위한 표준안에서 사용되는 루트 인증기관은 통상 최종개체가 믿는 또는 자신이 인증서를 발급받는 인증기관을 의미하며, 공개키 기반구조에서 루트 인증기관과는 다른 의미로 사용되고 있다.

인증서 관리 프로토콜을 위한 구성 시스템은 그림 1와 같이 최종개체에게 인증서를 발행하는 인증기관(CA : Certification Authority), 인증기관의 일부 기능인 신분확인 기능을 대신하는 등록기관(RA : Registration Authority), 인증기관에게 인증서 발행을 요구하고 발행된 인증서를 수신하는 최종개체(EE : End Entity), 그리고 인증서와 인증서 취소 목록을 저장하는 저장소(Repository)들로 구성된다. 인증서 관리 프로토콜은 이들 구성 요소간의 인증서 관리를 위하여 요구되는 다양한 기능과 이를 위한 메시지 형식을 정의하고 있다. 그림 1에서 초기 인증키와 참조값은 인증서 발급시에 필요한 비밀정보로써, 관리 메시지와 무결성과 기밀성을 제공하기 위하여 최종개체의 신분확인, 초기인증키 및 참조값을 포함하고 있는 스마트카드 형태의 토큰의

분배, 최종개체를 위한 인증서의 취소요구, 최종개체에 X.500 DN(Distinguished Name)이 할당, 최종개체를 위한 암호키 생성, 키 쌍의 보관 등의 업무를 수행하는 개체이다. 등록기관이 필요한 기술적 이유는 최종개체와 인증기관이 지리적으로 멀리 떨어져 있는 경우, 모든 최종개체가 하드웨어 토큰을 초기화시킬 수 있는 장치를 포함하고 있지 않고 등록기관에 이를 설치하여 초기화하도록 하는 경우, RA가 최종개체를 대신하여 서명된 인증서 취소 요구를 하여야 하는 경우 등이 있다. 등록기관이 필요한 관리적 이유는 토큰 초기화 기능을 모든 최종개체에 두는 방법보다는 RA에 두는 것이 경제적으로 유리하며, RA의 구축이 인증기관의 수를 줄일 수 있는 것이다

2. PKI 관리 요구 사항

이 프로토콜은 PKI 관리를 위한 다음과 같은 요구사항을 만족해야 한다.

① PKI 관리는 ISO 9594-8 표준과 관련 부속 표준과 순응해야 한다.
② PKI 관리는 PKI 관리의 다른 표준안들과 순응해야 한다.
③ PKI 관리 프로토콜은 RSA, DSA, MD5, SHA-1 등의 다른 산업계 표준 암호 알고리듬들의 사용을 허용해야 한다.
④ PKI 관리 프로토콜은 관련 최종 개체, RA, 또는 CA에 의한 키쌍의 생성을 배제해서는 않된다. 키쌍은 어디서도 생성될 수 있다.
⑤ PKI 관리 프로토콜은 관련 최종개체, RA, 또는 CA에 의한 인증서의 공표를 지원해야 한다. 다른 실현방법과 다른 환경들은 그들 중 한가지에 의한 공표 방법을 지원해야 한다.
⑥ PKI 관리 프로토콜은 최종개체가 인증서의 취소를 요구를 허용하게 함으로써 인증서 취소 목록의 생성을 지원해야 한다.
⑦ PKI 관리 프로토콜은 메일, ftp, http, tcp/ip 등의 다양한 전달 메커니즘을 사용할 수 있어야 한다.
⑧ 인증서 생성의 최종 권한은 인증기관에 존재한다. 인증기관은 운영정책에 따라 인증서 필드 값을 변경할 수 있고 확장 필드의 값을 부가, 삭제, 변경할 수 있다. 다시 말하면 모든 최종개체들은 요구된 그것과 다르게 발행된 인증서의 처리를 수행할 수 있어야 한다. 예를 들어 인증기관은 최종개체가 요구하는 유효기관을 짧게 만들 수 있다. 인증서 정책은 요구 개체가 새로 생성된 인증서를 검토하고 수락한 후에 인증서를 공표하고 분바하도록 규정할 수 있다.
⑨ 비타협된(non-compromised) 인증기관 키쌍의 새로운 인증기관 키쌍으로의 계획된 전환은 반드시 지원되어야 한다. 인증기관의 키가 타협된다면 인증기관의 영역내에 존재하는 모든 최종개체들은 재초기화 과정을 수행해야 한다.
⑩ 자신의 PSE에 새로운 인증기관 공개키를 포함하고 있는 최종개체는 옛 공개키를 이용하여 검증될 수 있는 인증서를 검증할 수 있어야 한다. 옛 인증기관의 키쌍을 믿고 있는 최종개체는 새로운 인증기관의 개인키로 서명된 인증서를 검증할 수 있어야 한다. 예를 들어 옛 인증기관의 공개키가 최종개체의 암호장치에 hardwired되어 있는 경우 유용하다.
⑪ RA의 기능은 어떤 실현이나 환경에서는 CA 자신에 의하여 수행될 수 있다. 프로토콜은 최종개체가 자신이 통신하는 주체가 인증기관이든 등록기관이든 무관하게 동일한 프로토콜을 사용할 수 있도록 설계되어야 한다.
⑫ 최종개체가 주어진 공개키를 포함하는 인증서를 요구하는 경우에, 최종개체는 공개키에 대응되는 개인키를 소유하고 있다는 사실을 보여 줄 수 있어야 한다. 이 것은 인증 요구의 유형에 따라 다르게 수행될 수 있다.

높은 수준에서 관리 메시지가 정의된 동작의 집합은 다음과 같이 그룹화 될 수 있다.

① 인증기관 설립: 새로운 인증기관이 설립될 때 초기 CRL의 생성과 인증기관 공개키의 수출을 포함하는 몇 가지 관리 단계들이 요구된다.
② 최종개체 초기화: 이는 루트 인증기관의 공개키를 수입하고 PKI 관리 개체에 의해 지원되는 선택사항들에 관한 정보의 요청을 포함한다.
③ 인증: 여러 동작들이 새로운 인증서의 생성을 초래한다.

◦초기등록/인증(Initial registration/certification):

최종개체가 인증기관이 그 최종개체를 위한 인증서를 발행하기 이전에 처음으로 인증기관이나 등록기관에 알려지는 과정이다. 이 과정의 최종 결과는 성공적인 경우 인증기관이 최종개체의 공개키를 포함하는 인증서를 발행하고, 최종개체로 발행된 인증서를 되돌려 주거나 공개 저장소로 발행된 인증서를 주게 된다. 이 과정은 최종개체 장치의 초기화를 포함하는 여러 과정들을 포함할 것이다. 예를 들어, 최종개체 장치는 인증경로를 검증하는데 이용되는 인증기관의 공개키로 안전하게 초기화되어야 한다. 여기에 더하여 최종개체는 자신의 키쌍으로 초기화되어야 한다.

- 키쌍 갱신(Key pair update): 최종개체의 키쌍은 주기적으로 갱신되어야 한다. 그리고 새로운 인증서가 발행되어야 한다.
- 인증서 갱신: 인증서가 유효기간이 경과하면 인증서는 새로 발급되어야 한다.
- 인증기관 키 쌍 갱신: 최종개체에서와 같이 인증기관 키 쌍은 정기적으로 갱신되어야 한다.
- 상호인증 요구: 한 인증기관은 다른 인증기관으로 상호인증서의 발행을 요구할 수 있다. 상호인증서는 인증서 내에 주체 인증기관과 발행자 인증기관이 다르며, SubjectPublicKeyInfo 필드에 검증키를 포함하고 있는 인증서이다. 만약 두 인증기관이 서로 다른 관리영역에 존재하면 상호인증서는 영역간(interdomain cross certificate) 인증서로 불리고 동일한 관리영역에 존재하면 영역내 인증서(intradomain cross certificate)로 불린다. 상호인증서는 X.509 규격에서 정의된 용어인 인증기관 인증서(CA-certificate) 와 일치하다. 많은 응용에서 상호인증서는 특별히 제한하지 않으면 영역간 인증서와 동의어이다. 상호인증서의 발행은 양방향성이다. 이는 두 인증기관이 서로에게 상호인증서를 발행함을 의미한다.
- 상호인증서 갱신: 상호인증서에 적용된다는 것을 제외하면 일반 인증서의 갱신과 동일하다.

④ 인증서/인증서 취소목록 공표 동작: 약간의 PKI 관리동작은 인증서와 인증서 취소목록의 공표를 초래한다.

- 인증서 공표: 인증서 생성의 문제를 해결하고 나면 인증서를 공포하는 수단이 요구된다. PKIX에서 정의된 이 수단은 메시지와 운영프로토콜인 LDAP 프로토콜과 연관될 수 있다.
- 인증서 취소 목록의 공표: 인증서 공표와 동일하다.

⑤ 복구 동작: 최종개체가 자신의 PSE를 분실했을 경우, 어떤 PKI 관리동작이 사용된다.

- 키쌍 복구: 선택적으로 사용자의 키 요소(사용자의 복호용 개인키를 포함)들이 CA, RA, 또는 이와 관련된 키백업시스템에 백업될 수 있다. 개체가 패스워드나 키 체인 파일을 분실해서 백업된 키 요소를 복구하기를 원하면, 프로토콜을 교환하여 이 복구를 지원해야 한다.

⑥ 취소 동작 : 어떤 PKI 관리 동작은 새로운 인증서 취소 목록의 목록이나 인증서 취소 목록을 생성을 초래한다.

⑦ 취소 요구: 인가된 사람(authorized person)이 인증기관에 인증서의 취소를 요구하는 비정상적인 상황을 알린다.

⑧ PSE 동작: PSE 동작을 정의하는 것은 규격의 범위를 벗어난 것이므로 여기서는 그러한 동작의 근간이 되는 PKImessage 만을 정의한다.

온라인 프로토콜만이 위에서 정의된 동작을 실현하는 유일한 방법이 아니다. 모든 동작에 대하여 동일한 동작을 초래하는 오프라인 방법들이 존재한다. 따라서 온라인 방법만을 강제하지 않는다. 예를 들어 하드웨어 토큰을 사용하는 경우 많은 동작들이 물리적 토큰의 전달의 일부분으로 달성될 수 있다.

3. 관리의 가정 및 제한

가. 최종개체 초기화

최종개체가 PKI 관리 개체들을 다루기 위한 첫 번째 단계는 지원되는 PKI 기능에 관한 정보를 요청하는 것과 관련 루트 인증기관의 공개키의 사본을 안전하게 획득하는 것이다.

나. 초기등록 및 인증

최종개체가 초기등록과 인증을 수행하는 많은 방법이 존재한다. 인증기관이 실행하는 정책의 다양성과 발생 가능한 최종개체의 다양한 유형으로 인해 하나의 방법이 모든 상황에 적합할 수 없다.

지원되는 초기등록 및 인증 방법을 구분할 수 있다. 의문의 최종개체가 PKI와 이전에 사전 접촉이

없었다는 점에서 "초기" 라는 단어가 매우 중요하다. 최종개체가 이미 검증된 키를 가지고 있다면 간단한 대체 방법이 가능하다.

지원되는 기법을 정의함으로써, 어떤 것은 필수로, 어떤 것은 선택사항으로 정의할 수 있다. 필수사항은 실제 사용에서 충분히 많은 경우를 포함하고, 선택사항은 작은 빈도를 갖는 특별한 경우를 포함한다. 이런 방법으로 융통성과 쉬운 실현간의 균형을 달성한다.

다. 사용된 기준

초기등록 및 인증의 개시는 최종개체와 관련된 첫 번째 PKI 메시지가 생성되는 어디에서나 일어나는 것으로 간주한다. 실제 세계에서 초기 등록과 인증은 어디에서나 발생할 수 있다. 가능한 장소는 최종개체, RA, 또는 CA 등이다.

인증서를 요구하는 최종개체에 의하여 생성된 온라인 메시지를 인증되거나 되지 않을 수도 있다. 최종개체로부터의 인증기관이나 등록기관으로 향하는 메시지에 대한 출처(origin)는 반드시 인증되어야 한다. 이 규격에서는 출처 인증은 어떤 out-of-band 수단으로 초기 인증키인 비밀키와 초기 거래를 확인하는데 이용되는 참고값를 인증기관이나 등록기관이 발행하는 인증기관이나 등록기관에 의하여 수행되어야 한다. 초기 인증키는 관련 PKI 정보를 보호하기 위하여 사용된다. 초기 등록 및 인증을 온라인 최종개체에서 PK 로 향하는 메시지가 인증되는지 안 되는지에 따라 구분한다. PKI에서 최종개체로 향하는 메시지에 대한 인증은 반드시 요구되는 것은 아니다. 어떤 경우든 인증기관의 공개키가 최종개체의 장치로 설치가 완료되거나 별도의 수단으로 최종개체에 입력된 초기 인증키에 기반을 면 쉽게 실현될 수 있다. 초기등록 및 인증은 최종개체로부터의 메시지가 다른 out-of-band 수단(차후의 일련의 방문을 통하여)으로 인증된다면 안전하게 될 수 있다.

본 규격에서는 키생성은 키쌍의 공개키나 개인키가 PKIMessage에 처음으로 나타나는 어느 곳에서나 발생할 수 있다고 간주한다. 이는 집중화된 키 생성 서비스를 배제하는 것을 의미하지 않는다. 집중화된 키 생성 서비스에서는 실제 키쌍은 다른 곳에서 생성되어 전용 또는 표준화된 키 생성 요구/응답 프로토콜을 사용하여 최종개체, RA, 또는 CA로 전달되는 방법을 이용한다. 키생성을 위한 가능한 세 가지 가능한 장소는 최종개체, RA, 또는 CA가 존재한다.

최종개체를 위한 초기 인증서를 생성하고 나서, 최종개체가 인증서를 포함하고 있는 메시지를 성공적으로 수신했다는 것을 분명히 확인하게 함으로써 추가의 보증을 획득할 수 있다. 자연적으로 이 초기 메시지는 초기 인증키나 다음 수단으로 보호되어야 한다.

라. 필수 기법

위에서 정의된 기준은 많은 종류의 초기 등록 및 인증 기법을 허용한다. 본 규격은 아래에 정의된 두 가지 기법 가운데 호응 인증기관(conforming CA), 호응 최종개체, 호응 등록기관은 기본 인증 기법을 지원해야 하는 것을 요구한다. 두 가지 기법은 집중화된 기법과 기본 인증 기법으로 구분된다.

① 집중화된 기법 : 이 방법은 매우 간단한 방법이다.
- 초기화는 검증하는 인증기관(certifying CA)에서 일어난다.
- 어떤 온라인 메시지 인증도 요구되지 않는다.
- 키생성은 검증하는 인증기관에서 일어난다.
- 어떤 확증 메시지도 요구되지 않는다.

메시지 흐름 측면에서 보면 이 기법은 요구되는 메시지는 인증기관으로부터 최종개체로만 전달된다. 이 메시지에는 최종개체를 위한 전체 PSE를 포함해야 한다. 최종개체가 암호화된 암호문을 복호하고 수신된 메시지를 인증하기 위하여 어떤 별도의 out-of-band 수단이 요구된다.

② 기본 인증 : 이 방법은 다음과 같다.
- 초기화는 최종개체에서 일어난다.
- 메시지 인증이 요구된다.
- 키 생성은 최종개체에서 일어난다.
- 확인 메시지가 요구된다.

메시지 흐름 측면에서 기본 인증 기법은 그림 2과 같다.

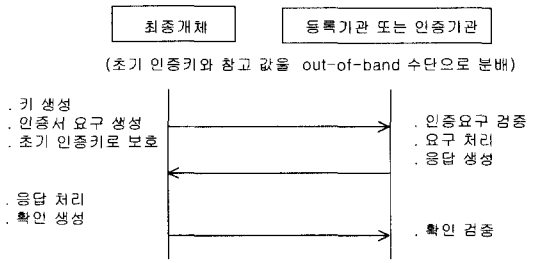


그림 2. 기본 인증 기법

확인 메시지에 대한 검증을 실패한 인증기관/등록기관은 이것이 공표 되었다면 새로 생성된 인증서를 취소해야 한다.

III. 필수 PKI 관리 기능들

인증서의 요구와 발급을 위하여 요구되는 인증서 요구 메시지와 인증서 분배를 위한 메시지의 대표적인 표준은 그림 3과 같이 각각 RKCS #10과 PKCS #7 표준안이다. 이 문서는 인증서 발급을 위하여 요구되는 신택스만 ASN.1 타입으로 기술하고 있으며, 실제로 PKI 관리 메시지가 전달되는 동안 보호되어야 할 추가의 메시지에 제한 형식은 정의하지 않고 있다.

그림 3. 인증서 발행과 분배를 위한 PKCS 표준안

1. 인증서 관리를 위한 주요 기능

인증서 관리 주요 기능은 인증기관을 설립하는 기능, 최종개체를 초기화하는 기능, 인증서를 발급 받는 기능, 발행된 인증서와 인증서 취소 목록(CRL : Certificate Revocation List)을 확인하기 위한 기능, 암호키의 분실이나 손상으로 인한 새로운 암호키를 복구하는 암호키 복구 기능, 그리고 생성된 인증서를 취소하기 위한 인증서 취소 기능 등이다.

① 인증기관 초기화 : 인증기관이 새로 설립될 때 인증기관은 자신의 초기 CRL을 생성하고, 자신의 공개키를 최종개체에 수출하는 등 관리 단계들이 요구된다.

② 최종개체의 초기화 : 최종개체는 자신에게 인증서를 발행해주는 자신이 신뢰하는 루트 인증기관의 공개키를 받아들이고 PKI 관리 개체에 의해 지원되는 선택사항 정보를 요청한다.

③ 인증 (Certification) : 인증 기능은 초기에 인증서를 발급 받는 과정, 최종개체에 암호키 갱신 및 이에 따른 인증서 갱신과정, 인증기관 인증서 갱신 과정, 인증기관간의 상호인증 과정과 상호 인증서 발급과정 등으로 구성된다.

- 초기등록/인증(Initial registration/certification) : 초기 등록 및 인증은 최종개체가 처음으로 인증서를 받는 경우 이용되는 관리 기능이다. 이 과정을 통하여 인증기관은 최종개체에게 인증기관의 공개키를 포함하는 인증서를 발행해주고, 최종개체는 발행된 인증서를 수신하고, 인증기관은 발행된 인증서를 공개 저장소에 저장하게 된다.
- 최종 개체 암호키 쌍 갱신(Key pair update) : 최종개체의 키쌍은 안전성을 위하여 주기적으로 갱신되어야 한다. 이는 최종개체가 주기적으로 새로운 인증서를 인증기관으로 발행 받아야 함을 위함이다.
- 최종개체 인증서 갱신 : 인증기관은 최종개체의 인증서의 유효기간의 경과하면 새로운 인증서를 발급해야 한다.
- 인증기관 암호키 쌍 갱신 : 최종개체의 인증서와 마찬가지로 인증기관의 암호키 상도 안전성을 위하여 정기적으로 갱신되어야 한다.
- 인증기관 사이의 상호인증 : 상호인증은 인증기관 사이에 믿음을 확장하는데 이용된다. 상호인증은 하나의 보안 영역(Security domain)에 있는 사용자와 또 다른 보안 영역에 있는 사용자간의 안전한 암호 통신의 수행을 가능케 한다. 하나의 인증기관은 다른 인증기관으로 상호 인증서 내에 주체 인증기관과 발행자 인증기관이 다르며, subject Public KeyInfo 필드에 검증키를 포함하고 있는 인증서이다. 만약 두 인증기관이 서로 다른 보안 영역에 존재하면 상호인증서는 영역간 상호인증서(Interdomain Cross-certificate)

로 불리고 동일한 관리영역에 존재하면 영역 내 인증서(Intradomain Cross-certificate)로 불린다. 상호인증서 발행은 양방향성이다. 이는 두 인증기관이 서로에게 상호인증서를 발행함을 의미한다.

◦ 인증기관간의 상호 인증서 갱신 : 상호인증서에 적용된다는 것을 제외하면 일반 인증서의 갱신과 동일하다.

④ 인증서 및 인증서 취소목록 공표 동작 : 인증기관과 최종개체는 발행된 인증서와 인증서 취소목록을 디렉토리나 데이터베이스를 이용해 공표해야 한다.

◦ 인증서 및 인증서 취소목록 공표 동작 : 인증기관과 최종개체는 발행된 인증서와 인증서 취소목록을 디렉토리나 데이터 베이스를 이용하여 공표해야 한다.

◦ 인증서 취소목록의 공표 : 인증서공표와 동일하다.

⑤ 개인키 복구 동작 : 최종개체가 자신의 PSE (Personal Security Enviroment)를 분실했을 경우를 대비하여 인증기관은 선택적으로 최종개체의 개인키를 복구하기 위한 관리 기능을 가져야 한다.

◦ 개인키 쌍 복구 : 최종개체의 암호와 서명을 위한 개인키를 CA, RA, 또는 이와 관련된 키백업시스템에 저장 될 수 있다. 개체가 패스워드나 키 체인 파일을 분실하여, 인증기관에 백업된 키 요소를 복구하기를 원하면, 인증기관은 키 복구 프로토콜을 이용하여 최종개체의 개인키를 복구할 수 있어야 한다.

⑥ 인증서 취소 동작 : 최종개체의 인증서는 개인키의 누설, 사용자의 소속 변경, 인증기관 개인키의 누설등 다양한 이유로 취소 될 수 있다. 인증기관은 최종개체와 인증기관 인증서의 취소를 위한 관리 기능을 가져야 한다.

◦ 취소 요구 : 인증서를 발급 받는 적법한 사용자, 이 사용자의 권한을 대리인에 의하여 인증기관에 의하여 발행된 인증서는 취소 될 수 있다. 이 요구는 발행된 인증서 취소 요구 메시지를 이용하여 실현 될 수 있다.

2. 인증서 발급을 위한 두 가지 초기 등록/인증 방법

초기 등록/인증 방법은 두 가지 방법이 있다. 하나는 최종개체의 개인키와 공개키의 상이 인증기관에 의하여 생성되는 집중화된 방식이고, 다른 하나

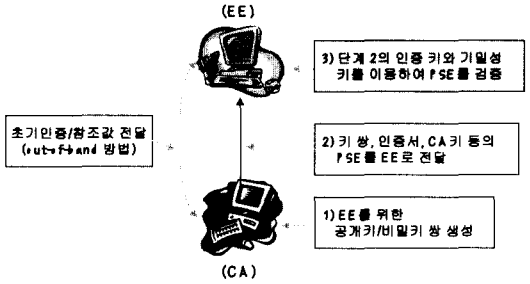


그림 4. 중앙집중 초기등록 및 인증과정

는 암호키 상이 최종개체에 의하여 생성되는 기본 인증 방법이다. 두 방식 공히 관리 메시지를 보호하기 위한 초기 인증키와 참조값을 안정한 방법으로 인증기관과 최종개체간에 공유하고 있어야 한다. 집중화된 기법의 경위, 인증기관은 최종개체를 위한 암호키 쌍을 생성하고, 그림 4와 같은 프로토콜을 최종개체와 수행한다. 이 과정을 통하여 최종개체는 자신의 인증서와 개인키를 갖게 된다.

인증기관은 최종개체로 키쌍 인증서, 그리고 인증기관의 공개키를 전달한다. 이 메시지에는 최종개체를 위한 전체 PSE 정보를 포함한다. 최종개체는 별도의 out-of-band 채널을 이용하여 최종체가 암호화된 암호문을 복호하고 수신된 메시지를 인증할 수 있는 초기 인증키와 참조값을 인증기관과 공유해야 한다. 최종개체가 자신을 위한 암호키 쌍을 생성하는 기본 인증 기법은 그림 5와 같은 절차를 따라서 인증서 발급을 위한 절차가 수행된다. PKIX에서는 기본 인증 기법의 사용을 권장한다.

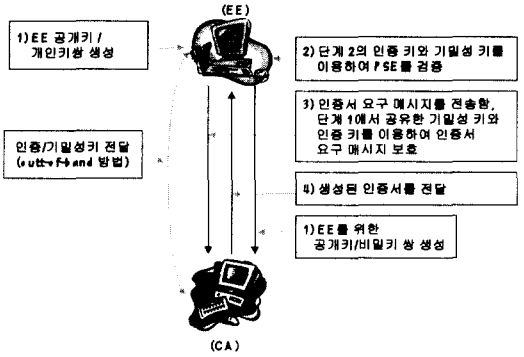


그림 5. 기본 인증 방법을 이용한 초기 등록 및 인증

최종개체는 그림 5와 같은 과정을 통해 인증서에 포함된 공개키에 대응되는 개인키를 소유하고 있음을 인증기관에게 증명 할 수 있다. 이 과정을 통하여 최종개체는인증기관으로부터 인증서를 발급받을 수 있다. 확인 메시지에 대한 검증을 실패한 인증기관은 이것이 공표되었다 하더라도 지금 새로 생성된 최종개체의 인증서를 인증서취소 목록을 이용하여 취소해야 한다.

3. 개인키 소유 증명

인증기관/등록기관이 개체와 공개키 간의 결합의 타당성에 대한 유효성을 검증하기 위하여 PKI 관리 동작은 최종개체가 인증서를 요구한 공개키에 대응되는 개인키를 소유하고 있다는 것을 증명하는 것이 가능하도록 해야 한다. 특정의 인증기관/등록기관이 어떻게 소유 증명을 수행할 것인지는 자유다. 그러나 인증기관/등록기관은 기존의 비-PKI 동작 프로토콜이 개체와 개인키간의 결합을 분명히 검사하지 않고 있으므로 반드시 개인키 소유 증명을 수행해야 한다. 인증기관이나 등록기관에 의해 결합이 검증되지 않는다면 인증서는 의미 없는 것이 될 것이다. 개인키 소유 증명은 인증서를 요청한 공개키의 종류에 따라 여러 방법으로 실행될 수 있다. 다중 용도로 사용되는 키가 사용된다면 적절한 개인키 소유 증명이 수행되어야 한다. 본 규격에서는 최종개체가 등록기관에 개인키 소유를 증명하고 등록기관이 다시 인증기관에 이 사실을 증언하는 경우를 허용한다. 예를 들어 인증되어야 할 서명키를 가지고 있는 최종개체는 등록기관에 적절한 서명문을 보내고 다시 등록기관이 이를 검증한 후 인증기관에 요구된 증명이 제공되었다는 것을 통보한다. 물론 이런 방식은 정책에 따라 허용되지 않을 수 있다. 즉, 인증기관만이 유일하게 인증하는 동안 개인키 소유 증명을 검증할 수 있다.

① 서명키 : 서명키를 위하여 최종개체는 개인키 소유를 증명하기 위하여 특정한 값을 서명할 수 있다.

② 암호키 : 암호키를 위하여 최종개체는 인증기관/등록기관에 개인키를 제공하거나 개인키의 소유를 증명하기 위하여 특정한 값을 복호하기를 요구받는다. 특정한 값을 복호하는 것은 직접적으로나 간접적으로 수행될 수 있다. 직접적인 방법은 인증기관이 난수를 생성하고 이를 암호키로 암호화하여 최종개체에 보내면 최종개체는 이를 복호한 난수를 응답으로 직접 전송할 것을 요구받는다. 간접적인 방법은 최종개체에게 암호화된 인증서를 발행한다. 최종개체는 이 암호화된 인증서를 복호하여 확인 메시지로 인증기관에 전달함으로써 복호할 수 있는 능력을 보인다. 이는 인증서를 특정의 최종개체만이 사용할 수 있는 형태로 인증서를 발행한다. 본 규격은 추가의 정보를 요구하지 않기 때문에 간접적인 방법의 사용을 권장한다. 즉, 소유 증명을 3가지 메시지를 이용하여 보여질 수 있다.

③ 키일치 키 : 키일치 키를 위하여 최종개체와 PKI 관리 개체는 최종개체가 개인키를 소유하고 있다는 것을 증명하기 위하여 공유된 비밀키를 확립해야 한다. 이는 특정의 인증기관에 의해 검증되는 키에 임의의 제한을 부여할 필요가 없다. 이는 최종개체가 임의로 Diffie-Hellman 파라미터를 선정하면 인증기관은

표 1. 인증서 관리와 관련된 RFC 문서

RFC 표준안	제목	주요내용	RFC 일시	비고
2510	Internet X.509 Public Key Infrastructure Certificate Menagement Protocol	- PKI 관리 기능 - PKI 관리 메시지	1999.3	표준트랙
2511	Internet X.509 CRMF (Certificate Request Message Formats)	- CRMF 신택스 정의	1999.3	표준트랙
2630	Crytographic Message Syntax	- 여러 암호학적 메시지타입 정의	1999.6	표준트랙
2314	PKCS #10 : Certificate Request Syntax Version 1.5	- 인증 요구 신택스	1998.3	표준트랙

단기적인 키쌍을 생성하여 공유된 비밀키를 생성할 수 있다.

4. 인증기관의 암호키 쌍의 갱신

인증기관이 자신의 서명용 키 쌍을 주기적으로 갱신 할 수 있어야 한다. 인증기관이 자신의 서명용 키를 갱신하고자 하는 경우, 인증기관은 두 개의 추가적인 cACertificate 속성 값을 생성해야 한다. 따라서 인증 기관은 전체적으로 OldWithOld, OldWithNew, NewWithOld, NewWithNew 등의 4가지 인증서 속성을 디렉토리에 공표해야 한다. 또한 인증기관은 서명요 키쌍을 변경하고자 하는 경우, out-of-band 수단으로 인증기관의 공개키를 획득한 최종개체들에게 전달해야 한다. 인증기관의 키를 변경하기 위해서는 인증기관 운영자는 다음의 절차를 수행해야 한다.

- 인증기관은 새로운 암호키 쌍을 생성한다.
- 인증기관은 새로운 개인키로 서명된 이전 공개키에 대한 인증서(oldWithNew 인증서)를 생성한다.
- 옛 개인키로 서명된 새로운 공개키에 대한 인증서(NewWithOld 인증서)를 생성한다.
- 인증기관은 위에서 생성된 인증서들을 디렉토리에 공표 한다.
- 인증기관은 최종개체가 out-of-band 수단으로 최종개체가 새 공개키를 획득할 수 있도록 한다.

과도 상태의 경우, 서명문 수신자는 네 가지 상태로 구분되어 서명문을 검증할 수 있다. 네 가지 서명자가 인증기관의 옛 서명키로 구한 인증서와 옛 서명용 개인키로 서명한 서명문을 송신하고 검증자가 새 공개키를 갖고 있는 경우, 서명자가 인증기관의 옛 서명키로 구한 인증서와 옛 서명용 개인키로 서명한 서명문을 송신하고 검증자가 옛 공개키를 갖고 있는 경우, 서명자가 인증기관의 옛 서명키로 구한 인증서와 옛 서명용 개인키로 서명한 서명문을 송신하고 검증자가 옛 공개키를 갖고 있는 경우, 서명자가 새 서명키로 서명된 인증서와 이를 서명문을 송신하고 검증자는 새 공개키를 갖고 있는 경우, 그리고 서명자가 새 서명키로 서명된 인증서와 이를 이용한 서명문을 송신하고 검증자는 새 공개키를 갖고 있는 경우 등으로 구분된다. 또한 저장소에 새 공개키에 대한 새 공개키와 옛 공개키를 소지하고 있는 경우에 따라 각각 2가지로 분류되어 전체 8가지 경우의 수가 나타나게 된다.

5. 인증서 관리 메시지의 구성

PKI 관리를 위한 메시지의 타입은 PKIMessage 이고, 다음과 같은 ASN.1 타입을 갖는다.

```
PKIMessage :: =SEQUEMCE {
   header              PKIHeader,
   body                PKIBody,
   protection[0]       PKIProtection OPTIONAL,
   exteraCertificate   SEQUEMCE SIZE (1..MAX)
                       of Certificate  OPTIONAL
}
```

PKIHeader는 PKI 메시지에 공통인 정보를 포함하고, PKIBody는 메시지에 한정되는(message-specific)정보를 포함하며, PKIProtectionvlfem는 PKI 메시지를 보호하는 비트를 포함한다. 그리고 extraCerts 필드는 수신자가 이용 가능한 인증서들을 포함한다. PKI 메시지 헤더는 송수신자의 주소와 처리를 확인하기 위한 부가 정보를 포함하고 있다. pvno 서브필드는 이 규격의 버전을 확인하는데 이용된다. sender 서브필드는 송신자의 이름을 포함한다. recipient 서브필드는 수신자의 이름을 포함한다. transactionID 서브필드는 응답을 수신한 수신자가 이전에 자신이 발행한 요구 메시지와 지금 수신한 이 메시지를 연결시키기 위하여 사용된다. 표 1는 인증서 관리와 관련된 RFC 문서를 기술한 것이다.

예를 들어, RAdml 경우, 주어진 시간에 보내진 많은 요구 메시지가 존재 할 수 있으므로, 등록기관은 응답의 transactionID 서브필드를 이용하여 특정의 요구를 확인하는데 요구된다. senderNonce와 receiveerNonce 서브필드는 재생 공격으로부터 메시지를 보호하는데 이용된다. messageTime 서브필드는 송신자가 메시지를 생성한 시간을 포함한다. freeText 서브필드는 사용자가 읽을 수 메시지를 수신자에게 전송하는 데 이용된다.

generalInfo 서브필드는 수신자에게 기계-처리가능(machine-processible)한 부가 데이터를 전송하는데 이용된다. PKI 메시지 바디부의 타입은 PKIBody로써, 일반적으로 초기화 요구, 초기화 응답, 인증 요구, 인증 응답, PKCS #10 인증서 요

구, pop 도전, pop 응답, 키 갱신 요구, 키 갱신 응답, 키복구 요구, 키복구 응답, 취소 응답, 상호 인증 요구, 상호 인증 응답, 인증기관 키 갱신 선언, 인증서 공표, CRL 공표, 확인 등의 메시지를 포함한다. PKI 메시지 보호부는 PKI 메시지의 무결성을 보장한다.

IV. 결론

본 논문에서는 IETF RFC 표준안을 근거로 하여 인증서 관리에서 요구되는 다양한 인증서 요구와 응답 메시지 신택스를 살펴보았다. 국내 공인 인증기관과 사용자간의 인증서 관리를 위해 프로토콜도 상기 표준안들에 근거하여 결정되어야 국제적인 또는 인증기관간의 호환성을 유지 할 수 있을 것이다. 또한 국내 공인 인증기관간의 상호 동작을 위하여 인증서 관리를 위한 국내 표준안의 개발이 요구된다.

참 고 문 헌

[1] IETF homepage, http://www.ietf.org/, 2000

[2] 이만영, 김지홍, 송유진, 염홍열, 이임영, 류재철, 전자상거래 보안기술, 생능, 1999.8.

[3] C. Adams, S. Farrell, Certificate Management Protocols, http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki3cmp-08.txt, 1998. 5

[4] RSA Data Security, Inc., Public Key Cryptography Standards #1-9, June 3, 1991.

[5] Diffie, M.E. Hellman: New Directions in Cryptography. IEEE Transactions on Information Theory. Vol.IT-22, 644-654, 1976.

[6] Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public Key Cryptosystems. Com ACM, Vol 21 No 2, 120-126, Feb 1978.

[7] ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on IT, Vol.IT-31, 469-472, 1985.

[8] ISO 7498-2(E): Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. First Ed. 1989-02-15.

[9] Generic Security Service Application Program Interface (GSSAPI), Version 2,06/22/1995, 〈draft-ietf-cat-gssv2-03.txt〉

[10] Generic Security Service API Version 2 : C-bindings,07/07/1995, 〈draft-ietf-cat-gssv2-cbind-01.txt〉

[11] The Simple Public-Key GSS-API Mechanism (SPKM),05/31/1995, 〈draft-ietf-cat-spkmgss-04.txt〉

[12] 염홍열, 이강석 "전자 상거래를 위한 공개키 기반 구조 제시" 1999.2

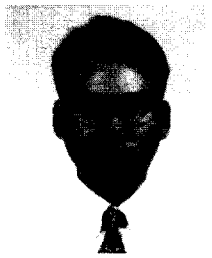
[13] 정보보호센터 홈페이지 연구자료들, http://www.kisa.or.kr/, 1999.

[14] Standards Australia, Strategies for the implementation of a public key authentication framework (PKAF) in Australia, 1996

〈著者紹介〉

류 종 호 (Jong-Ho Yu)

1998년 2월 순천향대학교 전자공학과 졸업
2000년 2월 순천향대학교 전자공학과 석사
2000년~현재 : 순천향대학교 전자공학과 박사과정
관심분야 : 전자지불, 암호이론



염 흥 열 (Heung-Youl Youm)

1981년 한양대학교 전자공학과 졸업
1983년 한양대학교 대학원 전자공학과 석사
1990년 한양대학교 대학원 전자공학과 박사
1982년~1990년 한국전자통신연구소 선임연구원
1990년~현재 순천향대학교 공과대학 정보기술공학부 부교수
1997년~2000년 순천향대학교 산업기술연구소 소장
2000년~현재 순천향대 산학연컨소시엄사업단 단장
1997년~현재 한국통신정보보호학회 총무이사
관심분야 : 전자상거래 보안, 공개키 기반 구조, 암호 이론, 부호이론, 이동통신보안
주관심분야 : 암호이론, 부호이론, 이동통신분야